

(●)

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 3月26日
Date of Application:

出願番号 特願2003-085547
Application Number:

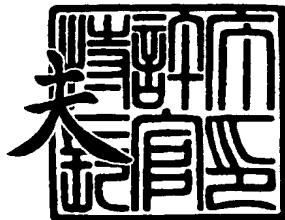
[ST. 10/C] : [JP2003-085547]

出願人 セイコーエプソン株式会社
Applicant(s):

2003年12月 5日

特許庁長官
Commissioner,
Japan Patent Office

今井康



【書類名】

特許願

【整理番号】

J0098171

【あて先】

特許庁長官殿

【国際特許分類】

G06T 17/00

【発明者】

【住所又は居所】 長野県諏訪市大和3丁目3番5号 セイコーホームズ株式会社内

【氏名】 長谷川 浩

【特許出願人】

【識別番号】 000002369

【氏名又は名称】 セイコーホームズ株式会社

【代理人】

【識別番号】 100095728

【弁理士】

【氏名又は名称】 上柳 雅裕

【連絡先】 0266-52-3528

【選任した代理人】

【識別番号】 100107076

【弁理士】

【氏名又は名称】 藤岡 英吉

【選任した代理人】

【識別番号】 100107261

【弁理士】

【氏名又は名称】 須澤 修

【手数料の表示】

【予納台帳番号】 013044

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0109826

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 原本性保証システム、情報埋め込み・改竄検出装置及び情報埋め込み・改竄検出方法並びに情報埋め込み・改竄検出プログラム

【特許請求の範囲】

【請求項 1】 複数の構造体データに情報を埋め込む情報埋め込み装置と、該情報埋め込み装置が情報を埋め込んだ複数の構造体データの改竄を検出する情報改竄検出装置とからなる原本性保障システムであって、

前記情報埋め込み装置が、

第1の規則に基づいて、前記複数の構造体データをソートするデータ標準化手段と、

該データ標準化手段がソートした複数の構造体データからなるビットストリームについて、所定のハッシュ関数を用いてメッセージダイジェストを算出するメッセージダイジェスト生成手段と、

該メッセージダイジェスト生成手段が算出したメッセージダイジェストをキーとして、前記データ標準化手段がソートした複数の構造体データを、前記第1の規則と異なる第2の規則でソートするデータ変換手段と

を具備し、

前記情報改竄検出装置が、

前記第1の規則に基づいて、複数の構造体データをソートするデータ標準化手段と、

該データ標準化手段がソートした複数の構造体データからなるビットストリームについて、前記ハッシュ関数を用いてメッセージダイジェストを算出するメッセージダイジェスト生成手段と、

該メッセージダイジェスト生成手段が算出したメッセージダイジェストをキーとして、前記データ標準化手段がソートした複数の構造体データを、前記第2の規則でソートするデータ変換手段と、

該データ変換手段がソートした複数の構造体データと、前記データ標準化手段がソートする前の複数の構造体データとを比較し、該複数の構造体データが一致すれば、前記データ標準化手段がソートする前の複数の構造体データが改竄され

ていないと判定し、該複数の構造体データが一致しなければ、前記データ標準化手段がソートする前の複数の構造体データが改竄されていると判定する判定手段と

を具備する

ことを特徴とするデータ原本性保障システム。

【請求項2】 所定の規則に基づいて、複数の構造体データをソートするデータ標準化手段と、

該データ標準化手段がソートした複数の構造体データからなるビットストリームについて、所定のハッシュ関数を用いてメッセージダイジェストを算出するメッセージダイジェスト生成手段と、

該メッセージダイジェスト生成手段が算出したメッセージダイジェストをキーとして、前記データ標準化手段がソートした複数の構造体データを、前記規則と異なる規則でソートするデータ変換手段と

を具備することを特徴とする情報埋め込み装置。

【請求項3】 情報埋め込み装置のデータ標準化手段と同一の第1の規則に基づいて、複数の構造体データをソートするデータ標準化手段と、

該データ標準化手段がソートした複数の構造体データからなるビットストリームについて、所定のハッシュ関数を用いてメッセージダイジェストを算出するメッセージダイジェスト生成手段と、

該メッセージダイジェスト生成手段が算出したメッセージダイジェストをキーとして、前記データ標準化手段がソートした複数の構造体データを、前記情報埋め込み装置のデータ変換手段と同一の規則であって、前記第1の規則と異なる規則でソートするデータ変換手段と、

該データ変換手段がソートした複数の構造体データと、前記データ標準化手段がソートする前の複数の構造体データとを比較し、該複数の構造体データが一致すれば、前記データ標準化手段がソートする前の複数の構造体データが改竄されていないと判定し、該複数の構造体データが一致しなければ、前記データ標準化手段がソートする前の複数の構造体データが改竄されていると判定する判定手段と

を具備することを特徴とする情報改竄検出装置。

【請求項4】 第1の規則に基づいて、複数の構造体データをソートし、該ソートした複数の構造体データからなるビットストリームについて、所定のハッシュ関数を用いてメッセージダイジェストを算出し、該算出したメッセージダイジェストをキーとして、前記ソートした複数の構造体データを、前記第1の規則と異なる第2の規則でソートすることを特徴とする情報埋め込み方法。

【請求項5】 請求項4に記載の情報埋め込み方法における第1の規則に基づいて、複数の構造体データをソートし、該ソートした複数の構造体データからなるビットストリームについて、所定のハッシュ関数を用いてメッセージダイジェストを算出し、該算出したメッセージダイジェストをキーとして、前記ソートした複数の構造体データを、前記情報埋め込み方法における第2の規則でソートし、該第2の規則でソートした複数の構造体データと、前記第1の規則に基づいてソートする前の複数の構造体データとを比較し、該複数の構造体データが一致すれば、前記第1の規則に基づいてソートする前の複数の構造体データが改竄されていないと判定し、該複数の構造体データが一致しなければ、前記第1の規則に基づいてソートする前の複数の構造体データが改竄されていると判定することを特徴とする情報改竄検出方法。

【請求項6】 第1の規則に基づいて、複数の構造体データをソートする処理と、

該ソートした複数の構造体データからなるビットストリームについて、所定のハッシュ関数を用いてメッセージダイジェストを算出する処理と、該算出したメッセージダイジェストをキーとして、前記ソートした複数の構造体データを、前記第1の規則と異なる第2の規則でソートする処理と、をコンピュータに実行させるための情報埋め込みプログラム。

【請求項7】 請求項6に記載の情報埋め込みプログラムをコンピュータが実行して行われるソート処理における第1の規則に基づいて、複数の構造体データをソートする処理と、

該ソートした複数の構造体データからなるビットストリームについて、所定のハッシュ関数を用いてメッセージダイジェストを算出する処理と、

該算出したメッセージダイジェストをキーとして、前記ソートした複数の構造体データを、前記情報埋め込み方法における第2の規則でソートする処理と、

該第2の規則でソートした複数の構造体データと、前記第1の規則に基づいてソートする前の複数の構造体データとを比較し、該複数の構造体データが一致すれば、前記第1の規則に基づいてソートする前の複数の構造体データが改竄されていないと判定し、該複数の構造体データが一致しなければ、前記第1の規則に基づいてソートする前の複数の構造体データが改竄されていると判定する処理と

、
をコンピュータに実行させるための情報改竄検出プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、主にデータ構造の記述方法について存在する冗長性を利用して情報を埋め込み、データの改竄や正当性を検出するための情報埋め込み・改竄検出装置及び情報埋め込み・改竄検出装置並びに情報埋め込み・改竄検出プログラムに関する。特に本発明は3次元グラフィックスやCAD等で生成される3次元設計データなど、3次元形状を記述したデータへ情報を埋め込む、データ・ハイディング技術、多面体や回転体等プリミティブな幾何学形状の組み合わせとして構成される3次元形状データの改竄や正当性を検出する技術に関する。

【0002】

【従来の技術】

従来、電子透かし技術、データ・ハイディング技術として、以下のようなものが知られている。

例えば、特許文献1には、3次元形状モデルの幾何パラメータを変更することにより情報を埋め込む技術について記載されている。

具体的には、この従来技術では3次元形状モデルの幾何パラメータ、すなわち、幾何形状を定義するための記述を変更することにより、種々の情報を前記3次

元形状モデルへ、可視または不可視の状態で埋め込む方法を採る。

埋め込み対象である3次元形状モデルは、通常、そのプリミティブ（構成要素）である、多面体、直線、点の集合、または曲面から構成される。また各プリミティブは幾何パラメータにより定義される。従って3次元形状モデルは多くの幾何パラメータの集合により、その全体の幾何形状が定義される。

よって、この従来技術では、3次元形状モデルを構成している複数のプリミティブの幾何パラメータを変更することにより、情報を埋め込むことが記載されている。

また、この従来技術では、幾何パラメータを数値パラメータ及び位相に分けて、各々を変更して情報を埋め込むこと、逆に、抽出は上記変更された幾何パラメータを検出することにより、埋め込まれた情報を取り出すことについて記載されている。

【0003】

また、特許文献2には、3次元形状モデルのデータにウェーブレット変換を施して、その結果に対して情報を埋め込む技術について記載されている。

具体的には、この従来例によれば、3次元形状変換手段が、オリジナルモデル V^0 のデータにウェーブレット変換処理を行い、電子透かし埋め込み手段が、ウェーブレット変換処理により生成されるWT係数ベクトルに透かしデータを埋め込んで、そのWT係数ベクトルに基づいて、3次元形状逆変換手段が、透かしデータを埋め込んだ3次元形状モデル（流通モデル V'^0 ）のデータを作成する。

したがって、この従来技術によれば、3次元形状データに、著作権情報等を含む電子情報データを埋め込む場合に、埋め込んだ3次元形状モデルの視覚的变化を考慮し、誤差の制御を行うことができ、また形状モデルの削除又は変形を受けた場合においても頑強な電子情報データ埋め込み方法について記載されている。

【0004】

【特許文献1】

特開平10-334272号公報

【特許文献2】

特開2000-82156号公報

【0005】

【発明が解決しようとする課題】

一方で、電子透かし技術、データ・ハイディング技術についての設計要求としては、

- ・ 透かし情報が編集、圧縮、伝送などの各種の処理に対して変質もしくは消失しないこと
- ・ 透かし情報の埋め込みに伴うコンテンツの劣化が最小限であること
- ・ ヘッダ部や特定の領域に集中せず、コンテンツ全域にわたり分散配置すること
- ・ 電子透かしの改ざんや消失などの悪意のある攻撃に対して強いこと
- ・ 透かし情報の埋め込み・検出処理が簡便で、処理所要時間が短いこと

等が挙げられるところ、上記先行技術文献1に記載の発明については、情報を埋め込むために本来の幾何データを変更する必要があること、透かし情報の検出アルゴリズムが複雑化することが問題となる。

また、上記先行上記先行技術文献2に記載の発明については、具体的な演算手法としてウェーブレット変換を用いることを特徴としているが、この発明の場合、元のデータとは異なるデータになってしまうことが問題となる。

【0006】

本発明は、このような事情を考慮してなされたものであり、その目的は、表現されているデータの「意味」、「品質」を全く変えずに、情報の埋め込み・読み出しが可能な情報埋め込み・改竄検出装置及び情報埋め込み・改竄検出装方法並びに情報埋め込み・改竄検出プログラムを提供することにある。

【0007】

【課題を解決するための手段】

この発明は上記の課題を解決すべくなされたもので、本発明は、複数の構造体データに情報を埋め込む情報埋め込み装置と、該情報埋め込み装置が情報を埋め込んだ複数の構造体データの改竄を検出する情報改竄検出装置とからなる原本性保障システムであって、前記情報埋め込み装置が、第1の規則に基づいて、前記複数の構造体データをソートするデータ標準化手段と、該データ標準化手段がソ

ートした複数の構造体データからなるビットストリームについて、所定のハッシュ関数を用いてメッセージダイジェストを算出するメッセージダイジェスト生成手段と、該メッセージダイジェスト生成手段が算出したメッセージダイジェストをキーとして、前記データ標準化手段がソートした複数の構造体データを、前記第1の規則と異なる第2の規則でソートするデータ変換手段とを具備し、前記情報改竄検出装置が、前記第1の規則に基づいて、複数の構造体データをソートするデータ標準化手段と、該データ標準化手段がソートした複数の構造体データからなるビットストリームについて、前記ハッシュ関数を用いてメッセージダイジェストを算出するメッセージダイジェスト生成手段と、該メッセージダイジェスト生成手段が算出したメッセージダイジェストをキーとして、前記データ標準化手段がソートした複数の構造体データを、前記第2の規則でソートするデータ変換手段と、該データ変換手段がソートした複数の構造体データと、前記データ標準化手段がソートする前の複数の構造体データとを比較し、該複数の構造体データが一致すれば、前記データ標準化手段がソートする前の複数の構造体データが改竄されていないと判定し、該複数の構造体データが一致しなければ、前記データ標準化手段がソートする前の複数の構造体データが改竄されていると判定する判定手段とを具備することを特徴とする。

【0008】

また、本発明は、所定の規則に基づいて、複数の構造体データをソートするデータ標準化手段と、該データ標準化手段がソートした複数の構造体データからなるビットストリームについて、所定のハッシュ関数を用いてメッセージダイジェストを算出するメッセージダイジェスト生成手段と、該メッセージダイジェスト生成手段が算出したメッセージダイジェストをキーとして、前記データ標準化手段がソートした複数の構造体データを、前記規則と異なる規則でソートするデータ変換手段とを具備することを特徴とする。

【0009】

また、本発明は、情報埋め込み装置のデータ標準化手段と同一の第1の規則に基づいて、複数の構造体データをソートするデータ標準化手段と、該データ標準化手段がソートした複数の構造体データからなるビットストリームについて、所

定のハッシュ関数を用いてメッセージダイジェストを算出するメッセージダイジェスト生成手段と、該メッセージダイジェスト生成手段が算出したメッセージダイジェストをキーとして、前記データ標準化手段がソートした複数の構造体データを、前記情報埋め込み装置のデータ変換手段と同一の規則であって、前記第1の規則と異なる規則でソートするデータ変換手段と、該データ変換手段がソートした複数の構造体データと、前記データ標準化手段がソートする前の複数の構造体データとを比較し、該複数の構造体データが一致すれば、前記データ標準化手段がソートする前の複数の構造体データが改竄されていないと判定し、該複数の構造体データが一致しなければ、前記データ標準化手段がソートする前の複数の構造体データが改竄されていると判定する判定手段とを具備することを特徴とする。

【0010】

また、本発明は、第1の規則に基づいて、複数の構造体データをソートし、該ソートした複数の構造体データからなるビットストリームについて、所定のハッシュ関数を用いてメッセージダイジェストを算出し、該算出したメッセージダイジェストをキーとして、前記ソートした複数の構造体データを、前記第1の規則と異なる第2の規則でソートすることを特徴とする。

【0011】

また、本発明は、情報埋め込み方法における第1の規則に基づいて、複数の構造体データをソートし、該ソートした複数の構造体データからなるビットストリームについて、所定のハッシュ関数を用いてメッセージダイジェストを算出し、該算出したメッセージダイジェストをキーとして、前記ソートした複数の構造体データを、前記情報埋め込み方法における第2の規則でソートし、該第2の規則でソートした複数の構造体データと、前記第1の規則に基づいてソートする前の複数の構造体データとを比較し、該複数の構造体データが一致すれば、前記第1の規則に基づいてソートする前の複数の構造体データが改竄されていないと判定し、該複数の構造体データが一致しなければ、前記第1の規則に基づいてソートする前の複数の構造体データが改竄されていると判定することを特徴とする。

【0012】

また、本発明は、第1の規則に基づいて、複数の構造体データをソートする処理と、該ソートした複数の構造体データからなるビットストリームについて、所定のハッシュ関数を用いてメッセージダイジェストを算出する処理と、該算出したメッセージダイジェストをキーとして、前記ソートした複数の構造体データを、前記第1の規則と異なる第2の規則でソートする処理とをコンピュータに実行させるための情報埋め込みプログラムである。

【0013】

また、本発明は、情報埋め込みプログラムをコンピュータが実行して行われるソート処理における第1の規則に基づいて、複数の構造体データをソートする処理と、該ソートした複数の構造体データからなるビットストリームについて、所定のハッシュ関数を用いてメッセージダイジェストを算出する処理と、該算出したメッセージダイジェストをキーとして、前記ソートした複数の構造体データを、前記情報埋め込み方法における第2の規則でソートする処理と、該第2の規則でソートした複数の構造体データと、前記第1の規則に基づいてソートする前の複数の構造体データとを比較し、該複数の構造体データが一致すれば、前記第1の規則に基づいてソートする前の複数の構造体データが改竄されていないと判定し、該複数の構造体データが一致しなければ、前記第1の規則に基づいてソートする前の複数の構造体データが改竄されていると判定する処理とをコンピュータに実行させるための情報改竄検出プログラムである。

【0014】

【発明の実施の形態】

以下、図面を参照して、本発明の情報埋め込み・改竄検出装置を適用したデータ原本性保障システムの第1の実施形態について説明する。本実施形態のデータ原本性保障システムは、複数の構造体データ（後述する）に情報を埋め込む情報埋め込み装置と、情報埋め込み装置が情報を埋め込んだ複数の構造体データの改竄を検出する情報改竄検出装置とから構成される。

図1は、本実施形態の情報埋め込み装置の構成を示す構成図である。

本実施形態の情報埋め込み装置は、制御部1と、入力部2と、出力部3と、記憶部4と、データ標準化処理部5と、付加情報付与処理部6と、メッセージダイ

ジェスト処理部7と、データ変換処理部8とをバス10で接続して構成される。

【0015】

制御部1は、入力部2、出力部3、記憶部4、データ標準化処理部5、付加情報付与処理部6、メッセージダイジェスト処理部7、データ変換処理部8におけるデータ入出力制御を行う。

入力部2は、透かし情報を埋め込む対象データである、複数の構造体データからなるオブジェクトの入力を受けるインターフェイス部である。

ここで、構造体データとは、1または複数のパラメータで記述されるデータ構造を持ったデータであって、該パラメータの値で順序付けることが可能なデータである。具体的には、データが複数のブロックに分かれて保持される形式の音声データ、図形形状等の記述データが複数のブロックに分かれて保持される形式の2次元画像データ、3次元画像データ、音声データ及び画像データが複数のブロックに分かれて保持される形式の動画像データ等であって、この順序を並べ替えてデータの持つ意味が変わらない構造となっているデータである。

【0016】

以下、3次元画像データとして、3次元グラフィックスやCAD等で生成される幾何形状データを例にとって説明する。3次元形状を記述するフォーマットとして、例えば

- ・VRML (Virtual Reality Modeling Language) Web等で用いられる3次元記述方式

- ・X3D (Extensible 3D) VRMLをXMLに統合した新しい記述形式
- ・DXF/DWG CADでデファクトスタンダードのフォーマット
- ・HPGL HPのグラフィックスフォーマット
- ・Raw Triangle ASCII TEXTで三角形の座標が書かれているだけのフォーマット

等がある。

【0017】

図2、図3に構造体データとして、3次元形状のオブジェクトを記述するフォーマットの一例を示す。図2は、x y z座標系で記述された6多角形のVRMLフォ

ーマットの例を示す。本発明の観点において、VRMLフォーマットは、x y z 座標値という1のパラメータで記述されるデータ構造を持ったテキストデータであって、このパラメータの値で順序付けることが可能なデータである（詳細は後述する）。

また、図3は、同様にx y z 座標系で記述された3角形のRaw Triangleフォーマットの例を示す。Raw Triangleフォーマットも、同様に、x y z 座標で記述される3つの点が1つの三角形を表す。

このように、オブジェクト記述フォーマットとは、オブジェクトの種類、大きさ、位置、向きを定める幾何パラメータからなる。

【0018】

出力部3は、透かし情報が埋め込まれた、複数の構造体データからなるオブジェクトを出力するインターフェイス部である。

記憶部4は、ヘッダ付加情報として、

- ・作成者や権利者を表す情報（名前、何らかのIDやメールアドレス、URL等）
- ・このデータを扱ったソフトウェアや装置に関する情報（シリアルナンバー ソフトウェアのバージョン情報等）
- ・作成日時やデータの大きさなどの情報

を記憶する。

【0019】

データ標準化処理部5は、所定の規則（以下、第1の規則とする）に基づいて、複数の構造体データをソートする。

ここで、データ標準化処理部5が用いる規則、つまり、ソートアルゴリズム及びその実装形態は、いくつかの手法が考えられるが、基本的には何らかの基準で並べ替えるという手法となる。

ソートアルゴリズムの適用対象、つまり、並べ替える対象としては、

- オブジェクト自身の記述内容を標準化する
- ファイル（ストリーム）内のオブジェクトの記載順序を標準化する

の2つがあり、それぞれについての具体的な実装例として、例えば以下の方法が考えられる。

【0020】

A. オブジェクトを構成する構造体データの記述内容の標準化

1). 例えばポリゴンのように、点の順序集合として表現される形式の構造体データであれば、どの点から記述を始めるかについて、順序を変更してもオブジェクトとしての意味は変更されてしまうということがない。したがって、この順序には自由度が存在する。すなわち、例えば、第1の規則として、予め任意に定めた基準点までの距離が最も近いもの、もしくは最も遠いものを記述開始点とすることが考えられる。

2). cylinder (柱) や回転体のようなデータ構造の場合は、軸を持っており、この軸は線分を表すデータによって記述される。すなわち、この記述内容にも同様に自由度が存在し、基点と方向ベクトルで記述する、もしくは、始端と終端の2点で記述することが考えられる。

【0021】

B. オブジェクトに順序を与える

1). オブジェクトから予め任意に定めた基準点までの距離の近い順、または遠い順に並べ替える。このとき、特定の座標についてのみ並べ替え処理を適用する、あるいは、所定の座標系に座標変換したものに対して、並べ替え処理を適用してもよい。つまり、座標系は直交座標系であるか否かを問うものではない。

また、距離を測定するオブジェクトの代表点（代表となるパラメータ値）の選択の方法の例として、例えば、

- ・オブジェクト記述において最初に現れる点
- ・オブジェクトの重心
- ・オブジェクトの中で、基準点に最も近い点（もしくは遠い点）

等が考えられる。

【0022】

2). オブジェクトの特性に応じた順序に並べ替える。

- ・たとえば、面オブジェクトならば面積、体積をもつオブジェクトならば体積でソートする。
- ・オブジェクトがテクスチャを持つようなものであれば、そのテクスチャ

を表現するデータに何らかの順序を定義し、それによってソートする。ここで言う「何らかの順序」とは、例えばテクスチャ表現データを数値であると解釈してその大きさによる順序を導入する、あるいはテクスチャ表現データを文字列であると解釈して辞書順による順序を導入する、等である。

3) オブジェクトの位置の相対関係による順序に並べ替える。

1つのオブジェクトを指定し、そのオブジェクトからの距離によってツリー状のデータ構造を構成する。そして、そのツリーを何らかのルールで辿るという手法によって順序付けを行う。

等が考えられ、かつ、これらを組み合わせることも考えられる。

【0023】

以下、標準化処理部5における標準化処理の例として、Raw Triangleの例を用いて説明する。

すなわち、まず3次元空間内に、特定の基準点Aを定義する（Step0）。次に、全ての三角形について、基準点Aに近いものから記述する形式に変換する（Step1）。つまり、Step1の過程は、三角形を1つ選択し、この選択した三角形を記述する3点それぞれから、基準点Aまでの距離を計算する。そして、距離が最も近い点が最初になるように、各点についての基準点Aまでの距離の大小関係に基づいて、三角形の記述を変更する。

次に、3次元空間内に、特定の基準点Bを定義する（Step2）。そして、Step1と同様に、全ての三角形について、基準点Bまでの距離を計算する。なお、距離計算の対象は三角形の記述の第1の点とする規則とする。そして、基準点Bまでの距離算出結果に基づいて、基準点Bまでの距離が近い順に、三角形を並べ替える。

【0024】

簡単な例について、上記第1の規則に基づく標準化処理の例を示す。

今、(0,0,0, 1,0,0, 0.1,0) という三角形T1、(0,1,0, 1,1,0, 1,2,0) という三角形T2について考える。RawEiangleフォーマットによる表記では、

.....

000100010

010110120

..... …表記1

という記述となる。たとえば基準点Aを (10, 0, 0) とすると、上記Step1により

、

三角形の記述は、

T1 (1, 0, 0, 0, 1, 0, 0, 0, 0)

T2 (1, 1, 0, 1, 2, 0, 0, 1, 0)

という順番となる（標準化A）。

【0025】

次に、基準点Bを (0, 10, 0) とすると、上記Step3, Step4により、T2のほう
がBに近いので、三角形の順番はT2が先となる。その結果、Raw Triangleの表記
は、上記の表記1から以下のように順序が並べ替えられる（標準化B）。

.....

110120010

100010000

..... …表記2

以上で「標準化」が完了する。すなわち、基準点A, Bが未知であれば、ソ
トアルゴリズムが既知であっても、正しく並べ替えることは不可能である。

また、距離の計算方法に関しても、例えば極座標や円筒座標系などに変換して
から重み付け距離計算を行う等の様々なバリエーションが考えられる。

【0026】

付加情報付与処理部6は、上記記憶部4に記憶された

- ・作成者や権利者を表す情報（名前、何らかのIDやメールアドレス、URL等）
- ・このデータを扱ったソフトウェアや装置に関する情報（シリアルナンバーや
ソフトウェアのバージョン情報等）

- ・作成日時やデータの大きさなどの情報

の付加情報を標準化処理部5の出力結果に付加する。なお、上記付加情報の内
容は埋め込む側・受け取る側双方で共通鍵としておく。

【0027】

メッセージダイジェスト処理部7は、データ標準化処理部5がソートした複数の構造体データからなるビットストリーム、または、さらに、付加情報付与処理部6がこれに付加情報を付加したビットストリームについて、所定のハッシュ関数を用いてメッセージダイジェストを算出する。

具体的なメッセージダイジェスト処理としては、例えば、1bit以上の任意のビット列を入力すると、固定長のビット列（160bitのビットパターン）が出力されるというMD5規格を用いる等が考えられる。

データ変換処理部8は、メッセージダイジェスト生成手段が算出したメッセージダイジェストをキーとして、データ標準化手段がソートした複数の構造体データを、上記第1の規則と異なる第2の規則でソートする。

【0028】

上記の例の続きで、標準化された表記2を出発点として記述順序を決定する第2の規則の例を示す。

.....

110120010

100010000

..... …表記2

まず標準化された複数の構造体データからなるビットストリーム、または、さらに、付加情報付与処理部6がこれに付加情報を付加したビットストリームについて、メッセージダイジェスト処理にかけたら、例えば以下のようないビット列（2進数表記）のメッセージダイジェスト値が得られたとする。

1110100110100011110000110101000111 · · ·

このビット列を用いて、表記2の記述をデータ変換する。

【0029】

A. 個々の三角形の頂点の記述順序の変換

まず上記のビット列を最初から2ビットずつ取得する。この場合、2bitであるので、4通りの組み合わせが考えられる。

最初の三角形T1の標準化された3頂点をT1a, T1b, T1cとすると、得られるビットに応じて、次のように並べ替えることとする。

00 : T1a, T1b, T1c
 01 : T1b, T1c, T1a
 10 : T1c, T1a, T1b
 11 : T1a, T1b, T1c

メッセージダイジェスト値の先頭の2ビットについて“11”であり、このままの並び替えを保持する。次の2ビットについて、“10”であり、2つ目の三角形に関して、頂点の記述順序を(c, a, b)の順に入れ替える。

【0030】

B. 三角形そのものの並べ替え

続いて、オブジェクト（この説明では三角形2個）の順番を決定する。なお、以下、より適切な例として、1つの実施例として、今、オブジェクトA, B, C, D, E, E, Gの7個について考えるが、三角形2個の場合でもまったく同様に適用可能であり、本発明は、これによって限定されるものではない。

すなわち、メッセージダイジェストの結果のビットストリームの続きは今、“100110”であり、これを左から順に使用することを考える。

最初： [A] B C D E F G

まず、先頭のオブジェクトAについて、先頭のbitが“1”なので、隣のBに入れ替える。なお、並べ替え操作対象のオブジェクトは[]で囲んだものである。

[1] : B [A] C D E F G

次のビットは“0”であり、今度は隣とは入れ替えずに操作対象となるオブジェクトを隣のCとする。

[2] : B A [C] D E F G

次も“0”であるので、さらに隣のDを操作対象とする。

[3] : B A C [D] E F G

次は“1”であるので、隣のEと入れ替える。

[4] : B A C E [D] F G

さらに“1”であるで、隣のFとも入れ替える。

[5] : B A C E F [D] G

最後は“0”であるで、並べ替えを終了する。

[6] : B A C E F D G

【0031】

以上で、データ変換処理部8による、メッセージダイジェスト値に基づく並べ替え処理が完了し、並べ替え処理された構造体データが出力部3に対して渡される。

すなわち、このようにしてメッセージダイジェスト関数が出力したビット列に従ってオブジェクトの記述順序を一意に決定することができる。

【0032】

図2は、本実施形態の情報改竄検出装置の構成を示す構成図である。

本実施形態の情報改竄検出装置は、制御部11と、入力部12と、出力部13と、記憶部14と、データ標準化処理部15と、付加情報付与処理部16と、メッセージダイジェスト処理部17と、データ変換処理部18と、改竄判定処理部19とをバス20で接続して構成される。

制御部11は、入力部12、出力部13、記憶部14、データ標準化処理部15、付加情報付与処理部16、メッセージダイジェスト処理部17、データ変換処理部18、改竄判定処理部19におけるデータ入出力制御を行う。

入力部12は、上記情報埋め込み装置によって、透かし情報が埋め込まれた、複数の構造体データからなるオブジェクトを入力するインターフェイス部である。

出力部13は、改竄判定処理部19による改竄の有無の判定結果（後述する）を出力するインターフェイス部である。

記憶部14は、上記情報埋め込み装置の記憶部4と同様と同一の付加情報を共通鍵として記憶する。

データ標準化処理部15は、データ標準化処理部5と同様に、上記第1の規則に基づいて、入力部12に入力される複数の構造体データをソートする。

付加情報付与処理部16は、上記情報埋め込み装置の付加情報付与処理部6と同様に、記憶部14が記憶する付加情報を標準化処理部5の出力結果に付加する。

メッセージダイジェスト処理部17は、データ標準化部15がソートした複数

の構造体データからなるビットストリームについて、ハッシュ関数を用いてメッセージダイジェストを算出する。

データ変換処理部18は、メッセージダイジェスト生成処理部17が算出したメッセージダイジェストをキーとして、データ標準化処理部15がソートした複数の構造体データ、または、さらに、付加情報付与処理部16によって、付加情報が付与された複数の構造体データを上記データ変換処理部8と同様に、上記第2の規則でソートする。

改竄判定処理部19は、データ変換処理部18がデータ変換した複数の構造体データと、データ標準化処理部15がソートする前の複数の構造体データとを比較し、これら2つの複数の構造体データが一致すれば、データ標準化処理部15がソートする前の複数の構造体データ、つまり、入力された複数の構造体データが改竄されていないと判定し、これら2つの複数の構造体データが一致しなければ、データ標準化手段がソートする前の複数の構造体データが改竄されていると判定する。

また、改竄判定処理部19は、データ変換処理部18がデータ変換した複数の構造体データについて、データ変換前に、付加データが付与されている場合は、これら2つの複数の構造体データが一致すれば、さらに、この付加データも改竄されていないと判定し、これら2つの複数の構造体データが一致しなければ、データ標準化手段がソートする前の複数の構造体データ、または、付加データのいずれか、あるいは、その両方が改竄されていると判定する。

【0033】

次に、図面を参照して、本実施形態のデータ提供システムの動作について説明する。図5は、本実施形態の原本性保障システムによる情報埋め込み処理の過程を示すフローチャートである。また、図6はこれに伴う情報改竄検出処理の過程を示すフローチャートである。

情報埋め込み処理として、情報埋め込み装置において、まず複数の構造体データからなるオブジェクトの集合である3次元形状モデルのデータを用意する。入力部2にこの3次元形状モデルのデータが入力されると、データ標準化処理部5は、予め定めた第1の規則でソートを行い、標準データ表現形式に変換する。

次に、付加情報付与処理部6 jは、ヘッダ情報、共通鍵等の付加情報を標準データ表現形式に変換された3次元形状モデルのデータに付与する。

次に、メッセージダイジェスト処理部7は、付加情報、標準化処理された3次元形状モデルのデータの全部または一部等についてメッセージダイジェスト処理を行ってメッセージダイジェスト値を得る。

データ変換処理部8は、このメッセージダイジェスト値のビットストリームに従って、第2の規則に基づいて、標準データ形式の表現を変換する。

以上で情報埋め込み処理が完了する。

【0034】

次に、情報改竄検出処理として、情報改竄検出装置において、情報が埋め込まれていると思われる3次元形状モデルのデータを用意する。入力部12にこの3次元形状モデルのデータが入力されると、データ標準化処理部15は、データ標準化処理部5と同様に、予め定めた第1の規則でソートを行い、標準データ表現形式に変換する。

次に、付加情報付与処理部16は、付加情報付与処理部6と同様にヘッダ情報、共通鍵等の付加情報を標準データ表現形式に変換された3次元形状モデルのデータに付与する。

次に、メッセージダイジェスト処理部17は、メッセージダイジェスト処理部7と同様に、付加情報、標準化処理された3次元形状モデルのデータの全部または一部等についてメッセージダイジェスト処理を行ってメッセージダイジェスト値を得る。

データ変換処理部18は、データ変換処理部8と同様に、このメッセージダイジェスト値のビットストリームに従って、第2の規則に基づいて、標準データ形式の表現を変換する。

改竄判定処理部19は、データ変換処理部18がデータ変換した複数の構造体データと、データ標準化処理部15がソートする前の複数の構造体データとを比較し、これら2つの複数の構造体データが一致すれば、データ標準化処理部15がソートする前の複数の構造体データ、つまり、入力された複数の構造体データが改竄されていないと判定し、これら2つの複数の構造体データが一致しなけ

れば、データ標準化手段がソートする前の複数の構造体データが改竄されていると判定する。また、改竄判定処理部19は、データ変換処理部18がデータ変換した複数の構造体データについて、データ変換前に、付加データが付与されている場合は、これら2つの複数の構造体データが一致すれば、さらに、この付加データも改竄されていないと判定し、これら2つの複数の構造体データが一致しなければ、データ標準化手段がソートする前の複数の構造体データ、または、付加データのいずれか、あるいは、その両方が改竄されていると判定する。

【0035】

したがって、本実施形態の原本性保障システムは、原本性保証の原理を利用して何らかのデータのハッシュ値をキーとしてオブジェクトの記述方法を変えることによって、データを表現する「冗長性」、すなわち、オブジェクトを記述する順序に情報を埋め込むので、表現されているデータの「意味」「品質」を全く変えることなく情報の埋め込みが可能となる。情報を陽に埋め込むのではなく、データの構造に意味がある。改竄した場合は適切な構造が変化するため、改竄を検出できる効果がある。

【0036】

以下、本実施形態のデータ提供システムのより詳細な動作の例について説明する。今、オブジェクト（プリミティブ）が三角形の集合であった場合を考える。なお、一般の多角形や回転体、任意の数式モデルで表現される幾何学モデルであっても同様に適用可能である。

例えば三角形T1～T100があったとし、それぞれの頂点をT1（T1_a, T1_b, T1_c）と表すこととする。ここでT1_a等は3次元ベクトルを表現している。

データ構造中で、T1からT100を記述する順序、また、三角形Tiにおいて頂点（Ti_a, Ti_b, Ti_c）を記述する順序には冗長性がある。最初に、例えば任意の基準点Aを考え、それぞれの三角形の重心ベクトルがAに近いものから順にソートする。

さらに、それぞれの三角形の頂点3つのうち、どれを最初に記述するかについても、例えば任意の基準点Bまでの距離が最も近いものを基点とするといった手法で、個々の三角形の記述方法も標準化する。

これによってデータが標準化される。

【0037】

次に、このデータに附属する付加情報（ヘッダに記載される）や秘密のビット列、または標準化されたデータそのもの、およびそれらの組み合わせから、メッセージダイジェスト関数を用いて特定の長さのビット列を得る。

【0038】

三角形の3頂点の記載する順序は3通り考えられるので、例えばメッセージダイジェストビットのbitごとに、どの頂点を最初に記述すべきかを決める。このようにして標準化されたデータの表現を変換する。

【0039】

ここで、基準点AやBの座標、またメッセージダイジェストを計算するための処理方法、ダイジェストを計算する際に用いるデータとして何を使うか、等を秘密にしておくことによって、改竄された場合に不正にデータを変換されることを防ぐことが出来る。

【0040】

上述の情報埋め込み装置、情報改竄検出装置は、内部に、コンピュータシステムを有している。

そして、上述した情報埋め込み、情報改竄検出に関する一連の処理の過程は、プログラムの形式でコンピュータ読み取り可能な記録媒体に記憶されており、このプログラムをコンピュータが読み出して実行することによって、上記処理が行われる。

すなわち、情報埋め込み装置、情報改竄検出装置における、各処理手段、処理部は、CPU等の中央演算処理装置がROMやRAM等の主記憶装置に上記プログラムを読み出して、情報の加工・演算処理を実行することにより、実現されるものである。

ここでコンピュータ読み取り可能な記録媒体とは、磁気ディスク、光磁気ディスク、CD-ROM、DVD-ROM、半導体メモリ等をいう。また、このコンピュータプログラムを通信回線によってコンピュータに配信し、この配信を受けたコンピュータが当該プログラムを実行するようにしても良い。

【図面の簡単な説明】

【図1】 本実施形態の情報埋め込み装置の構成を示す構成図である。

【図2】 x y z 座標系で記述された6多角形のVRMLフォーマットの例を示す図である。

【図3】 x y z 座標系で記述された3角形のRaw Triangleフォーマットの例を示す図である。

【図4】 本実施形態の情報改竄検出装置の構成を示す構成図である。

【図5】 本実施形態の原本性保障システムによる情報埋め込み処理の過程を示すフローチャートである。

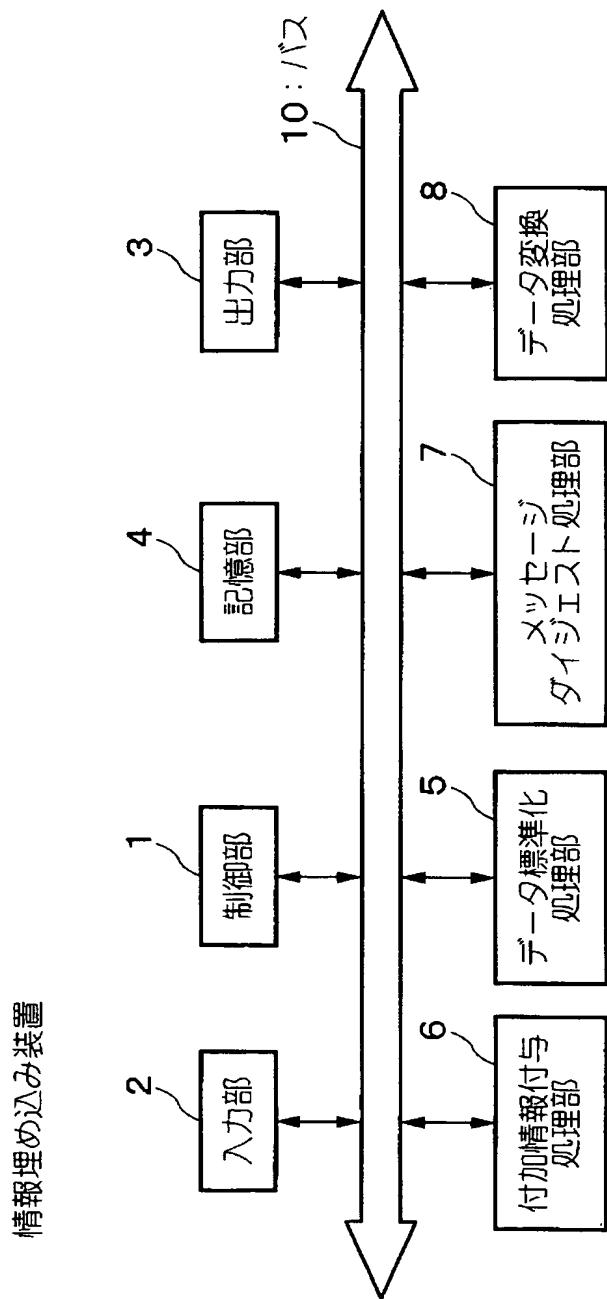
【図6】 情報改竄検出処理の過程を示すフローチャートである。

【符号の説明】

- 1、 1 1 …制御部
- 2、 1 2 …入力部
- 3、 1 3 …出力部
- 4、 1 4 …記憶部
- 5、 1 5 …データ標準化処理部
- 6、 1 6 …付加情報付与処理部
- 7、 1 7 …メッセージダイジェスト処理部
- 8、 1 8 …データ変換部
- 1 9 …改竄判定処理部

【書類名】 図面

【図 1】



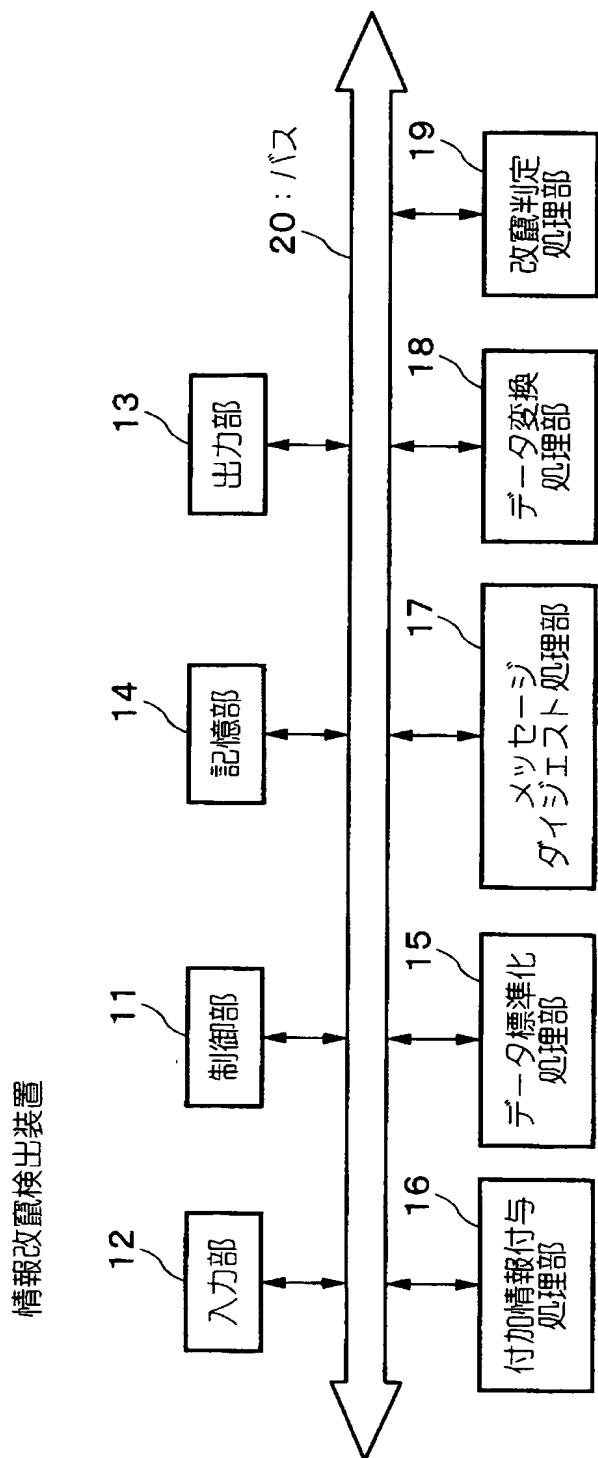
【図2】

```
…VRMLの例.....  
# VRML V1.0ascii  
Coordinate3 {  
    point [  
        020,  
        -101,  
        101,  
        10-1,  
        -10-1,  
        0-20  
    ]  
}  
IndexcdFaceSet {  
    coordIndex [  
        0,1,2,-1,  
        0,2,3,-1,  
        0,3,4,-1,  
        0,4,1,-1,  
        5,1,2,-1,  
        5,2,3,-1,  
        5,3,4,-1,  
        5,4,1,-1  
    ]  
}
```

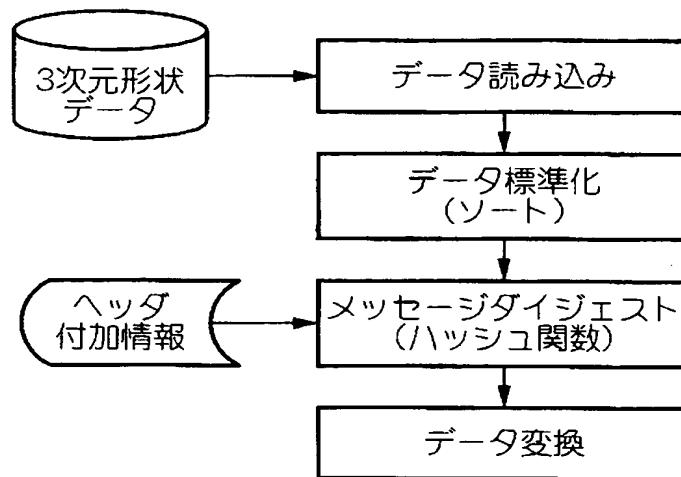
【図3】

```
…RawTriangleの例.....  
1. 0 -1. 1 0. 8  
3. 5 2. 7 6. 5  
4. 8 -2. 1 3. 3  
-1. 2 2. 1 -0. 9  
5. 3 -1. 1 -2. 8  
4. 1 1. 1 -0. 9
```

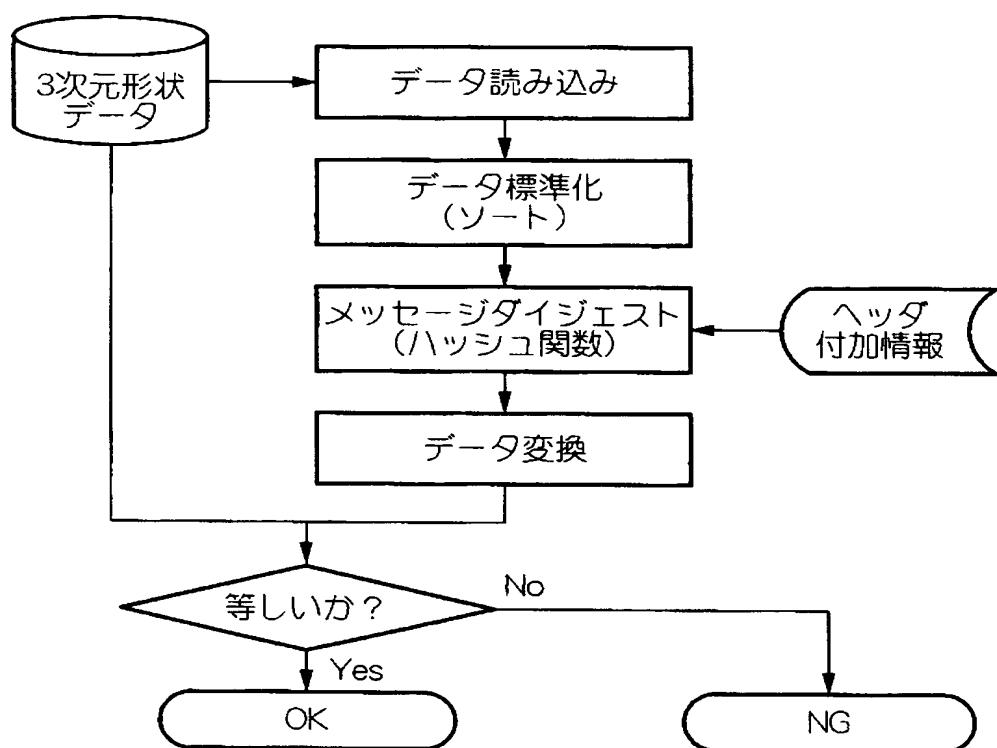
【図4】



【図5】



【図6】



【書類名】 要約書

【要約】

【課題】 表現されているデータの「意味」、「品質」を全く変えずに、情報の埋め込み・読み出しが可能な情報埋め込み・改竄検出装置及び情報埋め込み・改竄検出装置方法並びに情報埋め込み・改竄検出プログラムを提供する。

【解決手段】 情報埋め込み装置において、第1の規則に基づいて、複数の構造体データをソートし、ソート結果についてメッセージダイジェストを算出し、算出結果をキーとして、さらに、第1の規則と異なる第2の規則でソートする。

情報改竄検出装置において、第1の規則に基づいて、複数の構造体データをソートし、ソート結果についてメッセージダイジェストを算出し、算出結果をキーとして、さらに、第2の規則でソートする。このソート結果と、第1の規則に基づいてソートする前のデータとを比較して一致すれば、改竄無しと判定し、一致しなければ改竄有りと判定する。

【選択図】 図5

認定・付加情報

特許出願の番号 特願2003-085547
受付番号 50300493352
書類名 特許願
担当官 第四担当上席 0093
作成日 平成15年 3月27日

<認定情報・付加情報>

【提出日】 平成15年 3月26日

次頁無

特願2003-085547

出願人履歴情報

識別番号 [000002369]

1. 変更年月日 1990年 8月20日
[変更理由] 新規登録
住所 東京都新宿区西新宿2丁目4番1号
氏名 セイコーエプソン株式会社